IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCE

Appellant:	Justin Page
Serial No.:	09/557,252
Filed:	April 24, 2000
For:	SYSTEM AND METHODS AND COMPUTER PROGRAM FOR PREVENTION, DETECTION, AND REVERSAL OF IDENTITY THEFT
Examiner:	Alford W. Kindred
Art Unit:	2163 Confirmation No. 8465

APPENDIX A TO APPELLANT'S APPEAL BRIEF

PENDING CLAIMS SUBJECT OF THE APPEAL:

LISTING OF THE CLAIMS:

19. A method to detect unauthorized attempts to detect identity information of an individual, to reclaim identity information obtained without authorization, to detect inaccuracies in identity information and to prevent unauthorized access to identity information, the method comprising the steps of:

a. establishing a database of known private information of one or more individuals, wherein the known private information includes one or more of personal information, financial information, criminal information, and authorized users and storage of such information;

b. persistently scanning the Internet for stored private information of the one or more individuals stored in one or more other databases, wherein the persistently scanning occurs without requiring initiation through an action of the one or more individuals;

c. replicating the stored private information of the one or more other databases gathered from the step of persistently scanning to a secure replication database;

d. establishing indicia of unauthorized storage or use, or inaccuracies, of stored private information;

e. recording location information of the one or more other databases containing the stored private information;

f. comparing the known private information and the stored private information stored in the secure replication database; and

f. comparing the known private information and the stored private information stored in the secure replication database; and

g. notifying the one or more individuals when the indicia of unauthorized storage or use, or inaccuracies, of stored private information are detected.

20. The method as claimed in Claim 19 further comprising the step of blocking access to the stored private information.

21. The method as claimed in Claim 19 further comprising the step of reporting unauthorized use or storage of stored private information, inaccurate stored private information, or a combination of the two.

22. The method as claimed in Claim 19 wherein the database of known private information and the secure replication database form part of a common database.

23. The method as claimed in Claim 19 wherein the step of notifying is performed by establishing a graphical user interface for the one or more individuals to observe one or more indicators of private information usage or storage based on the established indicia.

24. The method as claimed in Claim 23 wherein the one or more indicators include a green light representation to show acceptable usage or storage, a yellow light to show potentially unacceptable usage or storage, and a red light to show unacceptable usage or storage.

25. The method as claimed in Claim 19 wherein the one or more other databases replicated include credit reporting service databases, court records databases, deed registry databases, and criminal record databases.

26. A system to detect and protect against unauthorized use or storage of an individual's personal information, or inaccuracies in such personal information, the system comprising:

a. a first database of known private information of one or more individuals;

b. means for persistently searching the Internet for one or more other databases containing stored private information of the one or more individuals, which means may be activated without initiation through an action by the one or more individuals;

c. a secure replication database of the stored private information copied from the one or more other databases containing the stored private information;

d. means for comparing the known private information of the first database with the stored private information of the secure replication database; and

e. notification means for notifying any of the one or more individuals when the obtained stored private information for such individual or individuals differs from the known private information, is stored in one or more of the one or more other database not authorized to have the stored private information, or a combination of the two.

27. The system as claimed in Claim 26 wherein the first database and the secure replication database form part of a common database.

28. The system as claimed in Claim 26 wherein the one or more other databases are substantially continuously searched for stored private information.

29. The system as claimed in Claim 28 wherein the means for searching is a search agent program selected from the group consisting of web spiders, bots, and robots.

30. The system as claimed in Claim 26 wherein the one or more other databases include credit reporting service databases, court records databases, deed registry databases, and criminal record databases.

31. The system as claimed in Claim 26 embodied in one or more computer programs.

32. The system as claimed in Claim 31 accessible through a computer interconnection system, wherein the one or more individuals providing the known private information may provide the known private information to the first database through the computer interconnection

system, and may further access the notification means through the computer interconnection system.

33. The system as claimed in Claim 32 wherein the notification means includes an interactive graphical user interface.

34. The system as claimed in Claim 26 further comprising an input device to enable the one or more individuals to report inaccurate private information, unauthorized usage of or access to the private information, or a combination of the two.

35. The system as claimed in Claim 26 further comprising a third database of one or more indicia of unauthorized storage or use of private information.

36. The system as claimed in Claim 35 wherein the third database is updatable and is accessed by the means for comparing to detect differences between the known private information and the stored private information, to detect unauthorized use or storage of the stored private information, or a combination of the two.